Installation security

4-4 minutes ⋮ 10/17/2024

There are several security matters to consider before and during the Qubes installation process.

Trusting your hardware

No operating system, not even Qubes, can help you if you're installing it on hardware that is already compromised. This includes CPUs, GPUs, SSDs, HDDs, the motherboard, BIOS/EFI/UEFI, and all relevant firmware. Unfortunately, in today's world of undetectable supply chain attacks, there are no easy solutions. (Tools like Anti Evil Maid (AEM) can help with *maintaining* the trustworthiness of your hardware, but not with establishing it in the first place.) Some users have chosen to use tools like Coreboot, Heads, and Skulls.

Verifying the Qubes ISO

You should verify the PGP signature on your Qubes ISO before you install from it. However, if the machine on which you attempt the verification process is already compromised, it could falsely claim that a malicious ISO has a good signature. Therefore, in order to be certain that your Qubes ISO is trustworthy, you require a trustworthy machine. But how can you be certain *that* machine is trustworthy? Only by using another trusted machine, and so forth. This is a classic problem. While various solutions have been proposed, the point is that each user must ultimately make a choice about whether to trust that a file is non-malicious.

Choosing an installation medium

So, after taking some measures to verify its integrity and authenticity, you've decided to trust your Qubes ISO. Great! Now you must decide what sort of medium on which to write it so that you can install from it. From a Qubes-specific security perspective, each has certain pros and cons.

USB drives

Pros:

- Works via USB, including with a USB qube.
- Non-fixed capacity. (Easy to find one on which the ISO can fit.)

Cons:

- Rewritable. (If the drive is mounted to a compromised machine, the ISO could be maliciously altered after it has been written to the drive.)
- Untrustworthy firmware. (Firmware can be malicious even if the drive is new. Plugging a drive with rewritable firmware into a compromised machine can also compromise the drive. Installing from a compromised drive could compromise even a brand new Qubes installation.)

Optical discs

Pros:

- Read-only available. (If you use read-only media, you don't have to worry about the ISO being maliciously altered after it has been written to the disc. You then have the option of verifying the signature on multiple different machines.)

Cons:

- Fixed capacity. (If the size of the ISO is larger than your disc, it will be inconvenient.)
- Passthrough recording (a.k.a., "burning") is not supported by Xen. (This mainly applies if you're upgrading from a previous version of Qubes.) Currently, the only options for recording optical discs (e.g., CDs, DVDs, BRDs) in Qubes are:
    1. Use a USB optical drive.
    2. Attach a SATA optical drive to a secondary SATA controller, then assign this secondary SATA controller to an app qube.
    3. Use a SATA optical drive attached to dom0.

    (Option 3 violates the Qubes security model since it entails transferring an untrusted ISO to dom0 in order to burn it to disc, which leaves only the other two options.)

Considering the pros and cons of each, perhaps a USB drive with non-rewritable (or at least cryptographically-signed) firmware and a physical write-protect switch might be the best option.